UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/799,921	03/10/2004	**Richard Dick**	10752.9	6824

21999 7590 12/31/2009

KIRTON AND MCCONKIE
60 EAST SOUTH TEMPLE,
SUITE 1800
SALT LAKE CITY, UT 84111

EXAMINER	
SHIFERAW, ELENI A	
ART UNIT	**PAPER NUMBER**
2436	

MAIL DATE	DELIVERY MODE
12/31/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/799,921	DICK, RICHARD	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 September 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10 and 12-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10 and 12-20 are pending.

Response to Amendment/Amendment filed on 09/25/2009

2. Applicant's arguments filed 09/25/2009 have been fully considered but they are not persuasive.

Regarding argument "no analysis has been previously provided regarding the specific features of dependent claims 3 and/or 9" argument is not persuasive as shown in the previous office action pages 5-11 the examiner clearly explained how the current application claims correspond with the other applications/patents. Claims 3 and/or 9 recite using web crawler programs to locate and retrieve publicly-available information regarding the individual from a plurality of Internet-access sources occurs automatically and claim 10 of the Patent No. 6,804,787 discloses automatically archived for a period of time set by a regulation and claim 1 discloses wherein the report includes: the requested healthcare information and any comments of the patient … that is equivalent. The other application 11057097 also gathers information.

Regarding applicant's argument "applicant notes that claim 15 has not been rejected. Applicant respectfully (in addition to those arguments that have been previously submitted) that the limitations of such claim are patentably distinct from the claims of 6804787 and 11057097, argument is not persuasive because it is the examiners understanding that the applicant agrees, see remark page 8 last line, that Web Crawler is noting but automatic gathering of information

since the applicant is arguing that the amended limitation on other independent claims, i.e., "using web crawler programs to locate and retrieve publicly-available information regarding the individual from a plurality of ...." is disclosed in claim 15 and claim 15 is actually disclosing "automatically gathering information …". Therefore the claim limitations of the current application are not patentably distinct from 6804787 and 11057097 claims limitations. Moreover the web crawler is taught by the applied reference Shelton discloses **WEBROBOT OR AUTOMATED SOFTWARE ROBOT for** automatic gathering information **(SEE col. 16 lines 64-col. 17 lines 12)** regarding an individual (patient) from plurality of information resources not controlled by the individual over a wide area computer network **(col. 3 lines 66-col. 4 lines 2, col. 9 lines 40-45, col. 5 lines 1-9 and fig. 1 elements 13 and 21; plurality of patients medical data stored in a database) and also the** Bjorksten (on par. 46 and figs 1-2) teaches "an automatic information collector for capturing personal information about user and automatically create or add to a file. Satyavolu **(see col. 4 lines 36-64, col. 2 lines 38-col. 4 lines col. 3 lines 65 and fig. 2)** teaches automatically gathering information regarding an individual from a plurality of information sources not controlled by the individual over a wide area computer network.

Regarding argument Bjorksten teaches "the use of automatic information collector for capturing personal information about a user" not presenting source of information to the user, argument is not persuasive because the master profile of Bjorksten that contains, eg. fig. 2, different sources of said information (Amazon(1), Amazon(2), citybank, ebanking.com... was presented to the user and the user changing the profile by checking/verifying which ones to keep or replace new and

also collects information automaticaly (par. 40-41, 48, 122, 99 and figs. 2, 8, and 16) and also the user is provided with address(s) of second party/stores webservers identifying information and grants access to the personal profile by sending an indication to the trusted party then to the second party/stores web servers (see par. 97-98).

With respect to argument on page 4 par. 1 of the previous office action the examiner continues to argue that the user profile as shown on fig. 2 is checked/verified by the user and changed via network fig. 1 (see par. 40-41, 48, 122, 99 and fig. 16). Bjorksten further teaches to annotate/change/adds data to the profile by viewing and checking/verifying which ones to keep or not (see par. 40, 48, 122, fig. 16, par. 30, 99 and claim 8). Since Bjorksten, as disclosed in this office action and argument, teaches maintaining information regarding sources of the information or accepting commentary on the information's accuracy, presenting the sources of the information and any commentary to other individuals.

Regarding argument Satyavolu failure teach "gathering information regarding an individual from a plurality of information sources that controlled by the individual from a plurality of information sources not controlled by the individual" argument is not persuasive because automated data gathering system in a plurality of connected users 145. Applicant's argument the mere use of the word "individual" in Satyavolu does not show equivalence between the teachings of Satyavolu and the invention as claimed is not certainly persuasive because it is disclosed that the user(s) information is automatically gathered.

Regarding argument Raveis failure to teach commentary including explanation of incorrect information in the database, argument is not certainly persuasive because it is disclosed clear enough to one ordinary skill in the art that in the cited portion comment is actually for an incorrect information/change.

The objections to claim 1 are withdrawn in view of the applicant's amendment.

3. Regarding Double patenting rejection, see above the examiner's explanation and rejection below. Moreover the examiner provided sufficient explanation to both double patenting rejections in the office action. The examiner corrects that on par. 8 of the previous office action to omit claim 11 as the applicant cancelled claim 11. The double patenting rejection of claims 1-13 is proper stating that they are not distinct from the other application. Copending application 11057097 claims similar limitations except "if the requested information is not subject to the requirement, releasing the requested information to the requestor" (see claim 1). However, Copending application claims, "determining whether the consent of the individual has been obtained, wherein the releasing of the requested information to the requestor is performed ...if the consent of the individual has been obtained when the consent is required" (see claim 1), which is equivalent to the instant application. Claims 1-13 of the instant application would have been obvious, to one ordinary skill in the art at the time of the invention was made over claims 1-24 of copending Application No. 11057097 because using a different equivalent word does not make the application invention distinct.

Every single limitation is addressed and reasonably rejected by the Office Action.

Regarding argument Raveis failure to teach accepting commentary on the ...., see the examiners explanation and argument above and rejection below.

Regarding argument Satuavolu failure to teach automatically gathering information regarding an individual see examiner's argument above and rejection below.

Regarding argument the references failure to teach "wherein the commentary on the accuracy of said information comprises an indication that a portion of said information is incorrectly associated with said individual" argument is not persuasive because the cited portion discloses if the second party device does not have permission to receive the information, then the second party with the second party device agree to a contract with the user regarding handling and use of the user's personal information within the service profile.

Response to Argument on 03/19/2009

4. Applicant's amendments and arguments are fully considered but are not persuasive for some and new grounds of rejection is/are presented for some.

Regarding the Double Patenting arguments, Examiner respectfully submits that the Office Action provided an analysis of the claims to support the rejection. Furthermore, the language of the patent is more specific than that of the instant application and therefore the claims are not patentably distinct. Moreover, both inventions are regarding managing

information (health data/personal information) of a person (patient/individual) securely and/or the person's information is released when the person authorizes the release ("request electronically authenticated to be authorized by the patient"/ "to not release information … without receiving authorization from said individual"). Therefore the nonstatutory obviousness-type double patenting rejection as being unpatentable over claims 1-19 of US patent 6804787 is appropriate and the rejection is maintained. Nevertheless, the instant and copending application are regarding managing data (business data/personal information) in compliance with privacy and release of data requires an approval ("determining whether the consent of the individual has been obtained, wherein the releasing of the requested information to the requestor is performed ...if the consent of the individual has been obtained when the consent is required"/ "if the requested information is not subject to the requirement, releasing the requested information to the requestor"). Therefore, argument is not persuasive, the nonstatutory obviousness-type double patenting as being unpatentable over copending application 11057097 is maintained.

Regarding argument Bjorksten failure to teach presenting said information and the sources of said information over the wide area computer network to said to individual to review and verify the information's accuracy" remark page 18, as recited in claim 15, is not persuasive because the master profile that contains, eg. fig. 2, different sources of said information (Amazon(1), Amazon(2), citybank, ebanking.com... was presented to the user and the user changing the profile by checking/verifying which ones to keep or replace new **(par. 40-41, 48, 122, 99 and figs. 2, 8, and 16) and also the user is provided with address(s) of second party/stores webservers identifying information and grants access to the personal profile**

by sending an indication to the trusted party then to the second party/stores webservers (see par. 97-98).

Regarding argument Bjorksten failure to teach accepting commentary on the accuracy of said the information based on the review from the individual over the wide area network computer" remark page 18 and 21, as recited in independent claims, argument is not persuasive because the user profile as shown on fig. 2 is checked/verified by the user and changed via network fig. 1 **(see par. 40-41, 48, 122, 99 and fig. 16). Argument Bjorksten does not teach "commentary on the accuracy" is not persuasive because Bjorksten does annotate/change/adds data to the profile by viewing and checking/verifying which ones to keep or not (see par. 40, 48, 122, fig. 16, par. 30, 99 and claim 8).**

Regarding argument Bjorksten failure to teach "presenting said selected portions of said information over said wide area computer network to said authorized individual along with identification of said sources of said selected portions of said information and any commentary on the accuracy of said selected portions of said information provided by said individual; and providing access to said database and said commentary to third parties" remark page 19, as recited in claim 15, argument is not persuasive because presenting said selected portions of said information over said wide area computer network **(fig. 1)** to said authorized individual **(see fig. 12)** along with identification of said sources **(eg. par. 0086)** of said selected portions of said information **(par. 97-98 and 40-41)** and any commentary **(par. 85, 97-98 and 40-46)** on the accuracy of said selected portions of said information provided by said individual **(97-98 and 40-46)**; and providing access to said database and said commentary to third parties **(par. 39-46, 97-98 and figs. 7-9 and 13A-B)**.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., In re Berg, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); In re Goodman, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); In re Longi, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); In re Van Ornum, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); In re Vogel, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and In re Thorington, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

6. A timely filed terminal disclaimer in compliance with 37 CFR 1.321 (c) or 1.321 (d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

7. Claims 1-10 and 12-20 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-19 of U.S. Patent No. 6,804,787.

8. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1-13 correspond to the claims 1-19 of the patent claims and encompass the scope of claims 1-13 of the instant application.

The differences are underlined as an example in claim 1. The differences are discussed. However the claims as a whole are equivalent.

Instant Application	Patent No. 6,804,787
1. A method for controlling a release of personal information comprising: depositing some personal information regarding an individual with a server; accepting commentary on the accuracy of said information based on review from saidindividual, wherein said commentary includes explanations of incorrect information on said server; obligating organizations that possess additional personal information regarding said individual to not disclose that additional personal information without authorization from said server; and instructing said server to not release said some personal information held on the server and to not authorize release of said additional personal information at the obligated organizations without receiving authorization from said individual. 2. Claim wherein the server is internet accessible. 3. (previously presented) The method of claim 1, further comprising using web crawler programs to locate and retrieve publicly-available information regarding said individual from a plurality of Internet-accessible sources 4. (original) The method of claim 1 wherein said individual is a member of a database service. 5. (original) The method of claim 1 wherein said personal information comprises database entries. 6. (original) The method of claim 1 wherein said obligated organizations are subscribers to a database service. 7. (currently amended) A method for creating a database of verified personal information comprising:	1. In a system that includes a computer device, a method for managing healthcare data in compliance with regulated privacy, security, and electronic transaction standards, the method comprising: receiving from a requestor a request for healthcare information relating to a patient, wherein any request is received through a single point of entry regardless of whether the request is from a requestor internal or external to a given healthcare facility; retrieving the requested healthcare information; assembling a report, wherein the report includes: the requested healthcare information; any comments of the patient received at a gatekeeper system regarding the requested healthcare information; and an audit trail; and transmitting a copy of the report to the requestor through a single point of exit regardless of whether the request was from a requestor internal or external to the given healthcare facility. 2. A method as recited in claim 1, wherein the request electronically authenticated to be authorized by the patient. 3. A method as recited in claim 1, further comprising the step for determining whether patient authorization exists for responding to the reques wherein if authorization from the patient has not been obtained, performing the step for obtaining authorization from the patient to provide the requested healthcare information. 4. A method as recited in claim 1, wherein the copy of the report includes patient specific healthcare information. 5. A method as recited in claim 1, further comprising the step for determining whether to provide de-identified healthcare information in response to the request, wherein if de-identified healthcare information is to be provided, performing the step for de-identifying the requested healthcare information. 6. A method as recited in claim 5, wherein the copy of the report includes de-identified healthcare information. 7. A method as recited in claim 1, further comprising the step for selectively performing a review of the report. 8. A method as recited in claim 1, further comprising the step for selectively encrypting the report. 9. A method as recited in claim 1, further comprising the step for selectively archiving the report.

gathering information regarding an individual; presenting said information over a wide area computer network to said individual to review and verify said information's accuracy; accepting commentary on the accuracy of said information based on said review from said individual over the wide area computer network, wherein said commentar7 includes explanations of incorrect information in said database; including said commentary in said database with said information; receiving a request over said wide area computer network from an authorized individual to review selected portions of said information; presenting said request to said individual for authorization; presenting said selected portions of said information over said wide area computer network to said authorized individual; and providing access to said database and said commentary to third parties. 8. (previously presented) The method of claim 7, wherein said wide area computer network is an internet. 9. (previously presented) The method of claim 7, wherein said the step of gathering information further comprises using web crawler programs to locate and retrieve publicly- available information regarding said individual from a plurality of Internet-accessible sources. 10. (original) The method of claim 7 wherein said individual is a member of a database service. 11. (canceled) 12. (original) The method of claim 7 wherein said third parties are subscribers to a database service. 13. (original) The method of claim 7 wherein said authorized individuals are members of a database service. 14. (previously presented) The method of claim 1, wherein obligating organizations that possess additional personal information regarding said individual to not disclose that additional personal information without authorization from said server comprises: receiving a disclosure from said individual at said server identifying said organizations that possess said additional personal information contacting said organizations that possess said additional personal information with said server; and receiving a contractual agreement from said organizations that possess said additional personal information to not release said additional personal information to third parties without first contacting said server for authorization.	10. A method as recited in claim 9, wherein the report is automatically archived for a period of time set by a regulation. 11. A system for managing healthcare data in compliance with regulated privacy, security, and electronic transaction standards, the system comprising: a computer system comprising: a gatekeeper system having: a single point of entry that is configured to selectively receive a request for healthcare information relating to a patient, wherein all requests are received through the single point of entry regardless of whether a requestor is internal or external to a given healthcare system facility; and a single point of exit that is configured to selectively provide a report in response to the request regardless of whether the requestor is internal or external to the given healthcare system facility, wherein the report includes the requested healthcare information relating to the patient, any comments of the patient received at the gatekeeper system regarding the requested healthcare information, and an audit trail; and at least one data source in communication with the computer system, wherein the at least one data sources comprises at least a portion of the requested healthcare information. 12. A system as recited in claim 11, wherein the computer system includes an interface engine. 13. A system as recited in claim 11, wherein the request is an electronic request. 14. A computer program product for implementing within a computer system a method for managing data in compliance with regulated privacy, security, and electronic transaction standards, the computer program product comprising: a computer readable medium for providing computer program code means utilized to implement the method, wherein the computer program code means is comprised of executable code for implementing the steps for: receiving from a requestor a request for healthcare information relating to a patient, wherein any request is received through a single point of entry regardless of whether the request is from a requestor internal or external to a given healthcare facility; retrieving the requested healthcare information; assembling a report, wherein the report includes: the requested healthcare information; any comments of the patient received at a gatekeeper system regarding the requested healthcare information; and an audit trail; and transmitting a copy of the report to the requestor through a single point of exit regardless of whether the request was from a requestor internal or external to the given healthcare facility. 15. A computer program product as recited in claim 14, wherein the computer program code means further comprises executable code for implementing the steps for: determining whether authorization from the patient exists for responding to the request; and if the authorization from the patient does not exist, obtaining electronic authorization from the patient to provide the requested information.

15. (currently amended) A method for creating and sharing a database of verified personal information comprising:
automatically gathering information regarding an individual from a plurality of information sources not controlled by the individual over a wide area computer network;
presenting said information and the sources of said information over the wide area computer network to said individual to review and verify said information's accuracy;
accepting commentary on the accuracy of said information based on said review from said individual over the wide area computer network;
including said commentary in said database with said information;
receiving a request over said wide area computer network from an authorized individual to review selected portions of said information;
presenting said request to said individual for authorization;
presenting said selected portions of said information over said wide area computer network to said authorized individual along with identification of said sources of said selected portions of said information and any commentary on the accuracy of said selected portions of said information provided by said individual; and
providing access to said database and said commentary to third parties.

16. (previously presented) The method of claim 15, further comprising:
supplementing said information regarding the individual by a continuous gathering process;
notifying said individual of updates to said information located by said continuous gathering process; and
accepting further commentary on the accuracy of said updates to said information from said individual over the wide area computer network.

17. (previously presented) The method of claim 15, further comprising:
receiving a search of said database from a third party that results in information about said individual being displayed to said third party; and
notifying said individual of said search and said display.

18. (previously presented) The method of claim 15, further comprising:
receiving additional information from said individual over the wide area computer network; and
receiving a designation from said individual designating said additional information as
one of:
information to be made available to all subscribers of said database; and information to be released only upon specific authorization of said individual.

19. (previously presented) The method of claim 15, wherein the commentary on the accuracy of said information

16. A computer program product as recited in claim 14, wherein th computer program code means further comprises executable code for implementing the steps for: determining whether to provide de-identified healthcare information in response to the request; and if de identified healthcare information is to be provided, de-identifying the requested healthcare information.

17. A computer program product as recited in claim 14, wherein th computer program code means further comprises executable code for implementing the step for selectively encrypting the report.

18. A computer program product as recited in claim 14, wherein th computer program code means further comprises executable code for implementing the step for selectively archiving the report.

19. A computer program product as recited in claim 14, wherein th computer program code means further comprises executable code for automatically implementing the step for archiving the report for a period of time set by a regulation.

comprises an indication that a portion of said information is incorrectly associated with said individual. 20. (previously presented) The method of claim 15, further comprising requiring said third parties to register with said database and present said database with identifying information prior to providing access to said database and to said commentary to said third parties.	

9. The instant application generally claims a method for controlling a release of personal information.

10. Patent 6,804,787 claims similar limitations except "health information", "a requester", "patient", "a single point entry/exit", and "request electronically authenticated to be authorized by the patient" (see claim 1).

11. However the instant application claims equivalent words/limitations: "personal information", "organizations", "individual", "server", and "to not release information ... without receiving authorization from said individual", respectively (see claim 1).

12. They are equivalent because in the instant application page 19 lines 4 discloses personal information including medical records. Page 19 paragraph 3-page 20 paragraph 2 discloses a requester being a medical organization. Fig. 2 discloses a user 100 that is patient to medical organizations 106 and/or third party insurance company 112. On page 20 paragraph 1, disclosed each of the organization contractually agrees to first contact enterprise/server 102 before releasing any information about the user so the server 102 can inform and request the user 100 if request to release confidential information is acceptable or not. On page 10 paragraph 2 the instant application discloses member/user/patient receiving an electronic alert, such as email, when information about the member is accessed or requested and on page 20 paragraph 1

disclosed when confidential information request is received the user must be contacted before releasing access.

13. Claims 1-13 of the instant application would have been obvious, to one ordinary skill in the art at the time of the invention was made over claims 1-19 of the patent 8404787 because using a different equivalent word does not make the application invention distinct.

14. Claims of the instant application therefore are not patentably distinct from the earlier patent claims and as such are unpatentable for obvious-type double patenting (In' re Goodman (CAFC) 29 USPQ2D 2010 (13/3/1993)).

15. Claims 1-13 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1-24 of copending Application No. 11057097.

16. Although the conflicting claims are not identical, they are not patentably distinct from each other because the instant case, all elements of claims 1-13 correspond to the claims of the copending claims and encompass the scope of claims 1-13 of the instant application.

17. The instant application generally claims a method for controlling a release of personal information.

18. The differences are discussed. However the claims as a whole are equivalent.

19. Copending application 11057097 claims similar limitations except "if the requested information is not subject to the requirement, releasing the requested information to the requestor" (see claim 1). However, Copending application claims, "determining whether the consent of the individual has been obtained, wherein the releasing of the requested information

to the requestor is performed ...if the consent of the individual has been obtained when the consent is required" (see claim 1), which is equivalent to the instant application.

20. Claims 1-13 of the instant application would have been obvious, to one ordinary skill in the art at the time of the invention was made over claims 1-24 of copending Application No. 11057097 because using a different equivalent word does not make the application invention distinct.

21. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 103

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> I'(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. Claims 15-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Bjorksten et al (US Patent Application Publication 2003/0097451, hereinafter Bjorksten) in view of Satyavolu et al. USPN 6517587 B2. and Raveis, JR. 20010047282 A1.

Regarding claim 15, Bjorksten teaches

a method for creating and sharing a database of verified personal information comprising **(abstract, and figs. 8 and 13A)**:

automatically gathering information regarding an individual from a plurality of information sources over a wide area computer network **(par. 46 and figs. 1-2)**;

presenting said information and the sources of said information over the wide area computer network to said individual to review and verify said information's accuracy **(par. 40-41, 48, 122, 97-99 and fig. 16; the user changing his profile shown on fig. 2 is by checking/verifying if he wants to keep the old profile or not)**;

accepting commentary on the accuracy of said information based on said review from said individual over the wide area computer network **(par. 40-41, 48, 122, 97-99 and fig. 16)**;

including said commentary in said database with said information **(par. 41-44 and 48, 122, 97-99 and fig. 16)**;

receiving a request over said wide area computer network from an authorized individual to review selected portions of said information **(par. 40, 97-99, figs. 8 and 16 and 127)**;

presenting said request to said individual for authorization **(par. 40-41, 97-99, figs. 8 and 16 and 127)**;

presenting said selected portions of said information over said wide area computer network to said authorized individual along with identification of said sources of said selected portions of said information and any commentary on the accuracy of said selected portions of said information provided by said individual **(par. 39-42, 97-99 and figs. 7-9 and 13A-B)**; and

providing access to said database and said commentary to third parties **(par. 41-46 and 97-99)**.

As the examiner understands, Bjorksten teaches the user browsing an internet web and accessing the web that gathers information regarding plurality of individuals and second party devices/stores as disclosed on before the user requests the trusted party and adds the second party/store address in the personal profile to be controlled by the user **(fig. 11 element 1102 and**

par. 85) but as the applicant amends and argues that Bjorksten fails to teach automatically gathering information regarding an individual from a plurality of information sources not controlled by the individual and the examiner combines **Satyavolu for teaching automatically gathering information regarding an individual from a plurality of information sources not controlled by the individual over a wide area computer network (see col. 4 lines 36-64, col. 2 lines 38-col. 4 lines col. 3 lines 65 and fig. 2).**

Therefore it would have been obvious to one ordinary skill in the art at the time of the invention was made to include the teachings of Satyavolu within the system of Bjorksten because they are analogous in data gathering profile database of a user and web access. One would have been motivated to include the teachings to provide different online information to the user and user protecting his personal information.

The combination fails to disclose the commentary including explanation of incorrect information in the database. However Raveis discloses changing data or updating data and commentary regarding the change and change date or on re-issue (see claim 64, par. 183-184, 164, and 175).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Raveis within the combination system because they are analogous in internet information sharing and personal information gathering. One would have been motivated to modify the teachings to provide reasoning why change is necessary and explain what, when and who made the changes. It is well known that commentary would explain things or reasons better.

Regarding claim 16, Bjorksten teaches

supplementing said information regarding the individual by a continuous gathering process **(par. 41-46)**;

notifying said individual of updates to said information located by said continuous gathering process **(par. 45-48)**; and

accepting further commentary on the accuracy of said updates to said information from said individual over the wide area computer network **(par. 45-49)**.

Regarding claim 17, Bjorksten teaches receiving a search of said database from a third party that results in information about said individual being displayed to said third party; and notifying said individual of said search and said display **(par. 61-64)**.

Regarding claim 18, Bjorksten teaches receiving additional information from said individual over the wide area computer network **(par. 61-64)**; and receiving a designation from said individual designating said additional information as one of: information to be made available to all subscribers of said database; and information to be released only upon specific authorization of said individual **(par. 40-42, 61-64)**.

Regarding claim 19, Bjorksten teaches wherein the commentary on the accuracy of said information comprises an indication that a portion of said information is incorrectly associated with said individual **(par. 67-70)**.

Regarding claim 20, Bjorksten teaches requiring said third parties to register with said database and present said database with identifying information prior to providing access to said database and to said commentary to said third parties **(par. 36-38 and 96-98)**.

24. Claims 1-6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shelton USPN 7,028,049 B1 in view of Coleman PG Pub 2004/0139025 A1. and Raveis, JR. 20010047282 A1.

Regarding claim 1, Shelton discloses

a method for controlling a release of personal information **(col. 4 lines 53-58, col. 8 lines 1-4, col. 3 lines 44-col. 4 lines 24 and col. 16 lines 32-63; controlling release of patient's confidential medical records by requiring patient's authorization anytime access is requested)** comprising:

depositing some personal information regarding an individual with an server **(col. 3 lines 66-col. 4 lines 2, col. 9 lines 40-45, col. 5 lines 1-9 and fig. 1 elements 13 and 21; plurality of patients medical data stored in a database....)**;

a web crawler **(WEB TOBOT)** programs to locate and retrieve publicly-available information regarding the individual from a plurality of internet-accessible sources **(SEE COL. 16 LINES 64-COL. 17 LINES 12; an automated software robot collecting data and storing in a master index from any record database connected to the web)**;

organizations **(col. 9 lines 9-18, col. 9 lines57-63, and fig. 1 elements 10a-c; health care info. users are clients, hospitals, doctors, nursing services, insurance companies...)** that possess additional personal information regarding said individual to not disclose that additional personal information without authorization from said server **(col. 7 lines 40-50, col. 10 lines 18-36, col. 9 lines 1-8, and col. l0 lines 53-col. 11 lines 45; physicians insurance companies 10b requiring patients confidential info. to be shared with authorized third-parties and server**

12, approval agent 16 requesting patient's approval first.., no medical document of the patient's is provided without patient's consent); and

instructing said server to not release said some personal information held on the server and to not authorize release of said additional personal information at the organizations without receiving authorization from said individual **(col. 11 lines 32-45, col. 8 lines 1-4; server 12~approval agent 16 is instructed not to release any patient's medical records stored in the database 21 and indexed in a master index 13 without first requesting patient's approval for release)**.

Shelton is silent about obligating organizations that possess personal information regarding said individual to not disclose that information without authorization from said enterprise/server.

However, Coleman discloses a method of controlling and/or protecting the privacy of individuals' personal information **(see abstract and fig. 2 element 420; protecting personal medical record) by obligating(col. 0041)** entities **(merchant, insurance companies, see par. 0030) to protect individuals' personal information (0056-0059 and fig. 3)** and providing individual generated restrictive notice to obligate entities **(par. 0031, 0056-0059)**, wherein said protect including obligation to entities not to share, transfer, and sell personal information to other entities **(par. 0027, 0059, and 0061)**.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Coleman within the system of Shelton because they are analogous in protecting personal confidential data. One would have been motivated to incorporate the teachings, of obligating organizations/entities not to disclose

individuals' confidential data, because it would restrict the organization/entities from sharing or transferring individuals confidential information without individual's permission.

The combination fails to disclose the commentary including explanation of incorrect information in the database. However Raveis discloses changing data or updating data and commentary regarding the change and change date or on re-issue (**see claim 64, par. 183-184, 164, and 175).**

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Raveis within the combination system because they are analogous in internet information sharing and personal information gathering. One would have been motivated to modify the teachings to provide reasoning why change is necessary and explain what, when and who made the changes.

Regarding claim 2, Shelton discloses the method, wherein said enterprise/server is Internet- accessible **(col. 9 lines 19-32 and lines 41-45)**.

Regarding claim 3, Shelton discloses the method, when using WebCrawler programs to locate and retrieve publicly-available information regarding said individual from a plurality of Internet-accessible sources occurs automatically **(col. 16 lines 64-col. 17 lines 12; web robot)**.

Regarding claim 4, Shelton discloses the method wherein said individual is a member of a database service **(col. 3 lines 66-col. 4 lines 2, col. 9 lines 40-45, col. 5 lines 1-9 and fig. 1 elements 13 and 21)**.

Regarding claim 5, Shelton discloses the method wherein said personal information comprises database entries **(col. 3 lines 66- col. 4 lines 2, and fig. 1 elements 13 and 21)**.

Regarding claim 6, Shelton discloses the method wherein said obligated organizations are subscribers to a database service **(col. 9 lines 57-col. 10 lines 4 and col. 5 lines 33-35)**.

Regarding claim 14, Coleman further teaches the method, wherein obligating organizations that possess additional personal information regarding said individual to not disclose that additional personal information without authorization from said server (0025-0032) and comprises:

receiving a disclosure from said individual at said server identifying said organizations that possess said additional personal information (**par. 0031, 0056-0059)**;

contacting said organizations that possess said additional personal information with said server **(par. 0027, 0059, and 0061)**; and

receiving a contractual agreement from said organizations that possess said additional personal information to not release said additional personal information to third parties without first contacting said server for authorization (0030, 0041, **0056-0061 and fig. 3)**. The rational for combining are the same as claim 1 above.

25. **Claims 7-10 and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shelton USPN 7,028,049 B1 in view of Adams et al. PG Pubs 2002/0013519 A1. and Raveis, JR. 20010047282 A1.**

Regarding claim 7, Shelton discloses a method for creating a database of verified personal information **(col. 4 lines 53-58, col. 8 lines 1-4, col. 3 lines 44-col. 4 lines 24 and col. 16 lines 32-63; controlling release of patient's confidential medical records of database 21 master index 13 by requiring patient 's verifying anytime access is requested)** comprising:

automatically gathering information (**WEBROBOT OR AUTOMATED SOFTWARE ROBOT SEE col. 16 lines 64-col. 17 lines 12)** regarding an individual (patient) from plurality of information resources not controlled by the individual over a wide area computer network **(col. 3 lines 66-col. 4 lines 2, col. 9 lines 40-45, col. 5 lines 1-9 and fig. 1 elements 13 and 21; plurality of patients medical data stored in a database)**;

receiving a request over said wide area computer network **(WAN see col. 9 lines 1-8)** from an authorized individual **(physicians/insurance companies 10b)** to review selected portions of said information **(col. 9 lines 57-col. 10 lines 36, and col. 10 lines 53-col. 11 lines 45; physicians/insurance companies 10b requesting patients confidential info.)**;

presenting said request to said individual (patient) for authorization **(col. 11 lines 31-45, col. 8 lines 1-4, and col. 10 lines 53-col. 11 lines 20; server 12 approval agent 16 indicating/presenting that a request has been made for the records selected by the requesting client 10 to the patient for authorization)**;

presenting said selected portions **(patient history, comprehensive medical records, lab reports, test results, prescription drug records.., see col. 7 lines 5-12)** of said information over said wide area computer network to said authorized individual **(physicians/insurance companies 10b) (col. 16 lines 32-63, col. 11 lines 4-53, col. 10 lines 18-35, and col. 7 lines 40-50)**; and

providing access to said database and said commentary **(patient consent/evidentiary documentation of the propriety)** to third parties **(insurance company/other doctor) (col. 7 lines 40-50, col. 6 lines 12-15, and col. 16 lines 32-63)**.

Shelton discloses presenting request to patients' medical record by email/fax. Shelton is silent regarding presenting said information over a wide area computer network to said individual (patient) to review and verify said information's accuracy; accepting commentary on the accuracy of said information based on said review from said individual over the wide area computer network; and including said commentary in a database with said information.

However Adams et al. discloses a secure patient test result delivery system **(see abstract)**. Patient is presented information over a wide area computer network **(par. 0015-0016)** to review and verify and information's accuracy **(par. 0085, 0095, 0109; patient logging online and editing patient database 560, that contain name, unique ID, phone number, address .... and editing to allow release of her/his information to physicians)**; patient accepting commentary **(checking release box, pars. 102-109)** on the accuracy of said information based on said review from said individual over the wide area computer network **(par. 0118; patient checking a medical release box via network for review by physicians)** and including said commentary in said database with said information **(0085, 0095, 0109 and 0118)**.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Adams et al. within the system of Shelton because they are analogous in patient medical data protection by requiring patients approval. One would have been motivated to do so because a patient would review and verify his/her information for editing/upgrading current info. and allowing or denying access to physicians.

The combination fails to disclose the commentary including explanation of incorrect information in the database. However Raveis discloses changing data or updating data and commentary regarding the change and change date or on re-issue (see claim 64, par. 183-184, 164, and 175).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Raveis within the combination system because they are analogous in internet information sharing and personal information gathering. One would have been motivated to modify the teachings to provide reasoning why change is necessary and explain what, when and who made the changes.

Regarding claim 8, Shelton discloses wherein said wide area computer network is an Internet **(col. 9 lines 19-32 and lines 41-45)**.

Regarding claim 9, Shelton discloses wherein said the step of gathering information further comprises using WebCrawler programs to locate and retrieve publicly- available information regarding said individual individuals from a plurality of Internet-accessible sources **(col. 16 lines 64-col. 17 lines 12; webrobot)**.

Regarding claim 10, Shelton discloses wherein said individual is a member of a database service **(Shelton col. 3 lines 66-col. 4 lines 2, col. 9 lines 40-45, col. 5 lines 1-9 and fig. 1 elements 13 and 21)**.

Regarding claim 12, Shelton discloses wherein said third parties are subscribers to a database service **(col. 7 lines 40-50)**.

Regarding claim 13, Shelt0n discloses wherein said authorized individuals are members of a database service **(col.9 lines 57-col. 10 lines 4 and col. 5 lines 33-35)**.

Conclusion

26. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

27. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 6:00am-2:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Primary Examiner, Art Unit 2436